IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Enrique David Sancho	Examiner: John M. Winter
Serial No.:	10/688,734	Group Art Unit: 3685
Filed:	Oct 16, 2003	Docket No.: 2062.001US3
Assignee:	iPass Inc.	
Title:	SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING	

APPELLANT'S BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Washington, D.C. 2023 1

This brief is presented in support of the Notice of Appeal filed on September 13, 2010, from the final rejection of pending claims 34-36, 40 and 43-44 of the above-identified patent application. The Office Action from which Appellant appeals was mailed 03/12/2010.

Please charge any required additional fees or credit overpayment to Deposit Account No. 50-3998.

Appellant respectfully requests reversal of the Examiner's rejection of pending claims 34-36, 40 and 43-44.

APPELLANT'S BRIEF ON APPEAL

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, iPass Inc...

2. RELATED APPEALS AND INTERFERENCES

Appellant knows of no other appeals or interferences which will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 1-33, 37-39, 41-42 have been cancelled. No claims are allowed. Claims 34-36, 40 and 43-44 have been finally rejected. Claims 34-36, 40 and 43-44 are pending, and are the subject of the present appeal.

4. STATUS OF THE AMENDMENTS

Claims 34-36, 40 and 43-44 are rejected on 03/12/2010. No further amendments were made. A Notice of Appeal was filed on September 13, 2010.

5. SUMMARY OF THE CLAIMED SUBJECT MATTER

This summary is presented in compliance with the requirements of Title 37 C.F.R. § 41.37(c)(1)(v), mandating a "concise explanation of the subject matter defined in each of the independent claims involved in the appeal ..." Nothing contained in this summary is intended to change the specific language of the claims described, nor is the language of this summary to be construed so as to limit the scope of the claims in any way.

Claim 34

Claim 34 is supported in Figure 8 and in the specification *inter alia* at paragraphs [0014] – [0015] and [0071] – [0073].

In Figure 8, a method for verifying a user and a user computer is illustrated. Paragraphs [0015], [0071] and [0073] describe receiving, at a first server, a first message from the user computer, the first message including a first computer fingerprint file identifying the user computer based on information associated with a plurality of components included in the user computer. Paragraphs [0015], [0071] and [0073] describe comparing the first computer fingerprint file against a second computer fingerprint file to verify the user computer, wherein the second computer fingerprint file includes information associated with the plurality of components included in the user computer, and the second fingerprint file being accessible by the first server. Paragraphs [0014], [0071] and [0073] describe receiving, at a second server, a second message from the user computer, wherein the second message includes a first identification for the user and the first identification is associated with the first computer

fingerprint file identifying the user computer. Paragraphs [0014], [0071] and [0073] describe comparing, at the second server, the first identification for the user against a second identification for the user to verify the user, wherein the second identification for the user is accessible by the second mini-server. Paragraphs [0015], [0066], [0067] and FIGS. 4-5 describe after the comparing of the first identification for the user against the second identification for the user to verify the user, generating a third message, at the second server, based upon the results of the comparison.

Claim 40

Claim 40 is supported in Figure 8 and in the specification *inter alia* at paragraphs [0014] – [0015] and [0071] – [0073].

In Figure 8, a system is illustrated that shows a vendor computer. Paragraphs [0015], [0071] and [0073] describe a first input unit configured to communicate with a first server and to receive a first server message containing information indicating that a user computer was verified by the first server based on a first computer fingerprint file identifying the user computer based on a plurality of components in the user computer. Paragraphs [0014], [0071] and [0073] describe a second input unit configured to communicate with a second server to receive a second server message containing information indicating that a user was verified, wherein the verification is based on a first identification for the user and the first identification is associated with the first computer fingerprint file identifying the user computer. Paragraphs [0015], [0066], [0067] and FIG. 5 describe a processor configured to receive the first server message from the

first input unit and the second server message from the second input unit and to authorize an action only if both the first server message contains information indicating the user computer was verified and the second server message contains information indicating the user was verified, wherein the first server and the second server are mini-servers, and wherein the first server message and the second server message are mini-server messages.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Are claims 34-36 and 43-44 properly rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter?

Is claim 40 properly rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention?

Are claims 34-36, 40 and 43-44 properly rejected under 35 U.S.C. 103(a) as being unpatentable over Pare Jr. et al. (US Patent 6,269,348) in view of Glass et al. (US Patent 6,332,193)?

7. ARGUMENT

A. §101 REJECTION OF THE CLAIMS

Claims 34-36 and 43-44 were rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

I. *THE APPLICABLE LAW*

"To properly determine whether a claimed invention complies with the statutory invention requirements of 35 U.S.C. 101, USPTO personnel must first identify whether the claim falls within at least one of the four enumerated categories of patentable subject matter recited in section 101 (i.e., process, machine, manufacture, or composition of matter)."[1] "The burden is on the USPTO to set forth a prima facie case of unpatentability. Therefore if USPTO personnel determine that it is more likely than not that the claimed subject matter falls outside all of the statutory categories, they must provide an explanation.

In *Bilski v. Kappos*, the Court held:

> Flook rejected '[t]he notion that post-solution activity, no matter how conventional or obvious in itself, can transform an unpatentable principle into a patentable process.' Id., at 590. The Court concluded that the process at issue there was "unpatentable under §101, not because it contain[ed] a mathematical algorithm as one component, but because once that algorithm [wa]s assumed to be within the prior art, the application, considered as a whole, contain[ed] no patentable invention." Id., at 594. As the Court later explained, Flook stands for the proposition that the prohibition against patenting abstract ideas "cannot be circumvented by attempting to limit the use of the formula to a particular

1 MPEP at § 2106 (IV)(B).

technological environment" or adding "insignificant postsolution activity." Diehr, 450 U. S., at 191–192.[2]

Also, the Court held that even though the machine-or-transformation test is not the sole test, this test is "a useful and important clue, an investigative tool, for determining whether some claimed inventions are processes under § 101."[3]

II. *DISCUSSION OF THE REJECTION OF CLAIMS 34-36 AND 43-44 UNDER 35 U.S.C. §101*

The Office Action indicated that claims 34-36 and 43-44 were rejected because

a §101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In addition, the tie to a particular apparatus, for example, cannot be mere extra-solution activity. See *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008).[4]

The Office Action further indicated claim 34 because the tie to an apparatus is "mere extra-solution activity" – referencing "receiving at a mini-server" in the claim. Applicant respectfully traverses. Claim 34 recites a process that is tied to multiple machines: a first server and a second server that are performing operations of the method claim that is beyond "extra-solution activity." Specifically, claim 34 includes at least four operations that are tied to an apparatus: 1) a first message is received at the first server; 2) a second message is received at the second sever; 3) the comparison between the two identification of the user are performed at the second server;

2 *Bilski v. Kappos*, 130 S.Ct. at 3230 (2010).
3 *Id.* at 3227.

and 4) a third message is generated at the second server based on the results of the comparison. Claim 34 is not reciting abstract ideas and tying mere extra-solution activity thereto. Rather, the method operations (receiving, comparing and generation) as recited therein are performed at different servers.

Therefore, Applicant submits that claims 34-36 and 43-44 recite patentable processes under 35 U.S.C. §101.

B. §112 REJECTION OF THE CLAIMS

Claim 40 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

I. *THE APPLICABLE LAW*

MPEP §2173.02 states:

> The essential inquiry pertaining to this requirement is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity. Definiteness of claim language must be analyzed, not in a vacuum, but in light of:
>
> (A) The content of the particular application disclosure;
>
> (B) The teachings of the prior art; and

4 Office Action at page 3.

> (C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made. In reviewing a claim for compliance with 35 U.S.C. 112, second paragraph, the examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph, by providing clear warning to others as to what constitutes infringement of the patent.[5]

MPEP §2173.05(p) states: "A functional limitation is an attempt to define something by what it does, rather than by what it is (e.g., as evidenced by its specific structure or specific ingredients). There is nothing inherently wrong with defining some part of an invention in functional terms. Functional language does not, in and of itself, render a claim improper. In re Swinehart, 439 F.2d 210, 169 USPQ 226 (CCPA 1971)."

II. *DISCUSSION OF THE REJECTION OF CLAIM 40 UNDER 35 U.S.C. §112*

The Office Action rejects claim 40 under 35 U.SC. §112 for indefiniteness for two different reasons.

First, the Office Action indicated that claim 40 is indefinite because "[c]laim 40 recites "message containing information indicating that a user was verified" however there is no corresponding structure in either the first or second input unit that implements any verification process, and is therefore indefinite." Therefore, the Office Action is requiring that some component (e.g., the first or second input units) implement the verification process in order for

5 MPEP §2173.02.

claim 40 to be definite. Applicant respectfully traverses. Under MPEP 2173.02, to comply with 35 U.S.C. 112, the claims are required to "set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity."[6] There is no requirement under 35 U.S.C. 112 that each operation be defined relative to what component performed such operation. In claim 40, the verification of the user occurred prior to the vendor computer receiving the first server message. Therefore, Applicant respectfully submits that this limitation is definite under 35 U.S.C. 112.

Second, the Office action indicated that claim 40 is indefinite because claim 40 is a "hybrid claim."

> Claim 40 is indefinite because it is a hybrid claim. In particular, the claim appears to be directed to neither a "process" nor a "machine," but rather embraces or overlaps two different statutory classes of invention. Evidence to support an interpretation that claim 17 is a product is (1) the preamble which states "a vendor computer" and (2) the body of the claim which recites "a first input unit .... " Alternatively, evidence that indicates the claim is directed to a process or method is the body of the claim which recites "to communicate with a second server to receive a second server message containing information indicating that a user was verified, based on a first identification for the user, generated using the first computer fingerprint file .... " Because of this conflicting evidence, it is unclear if claim 17 is a product or process claim. See the 35 U.S.C. §101 rejection above. See MPEP §2173.05(p) II or Ex Parte Lyell, 17 USPQ2d 1548 (B.P.A.I. 1990).7

As noted in the "Applicable Law" section above, the use of a functional limitation in a claim is proper. In particular, MPEP §2173.05(p) states: "[a] functional limitation is an attempt

6 *Id.*

to define something by what it does, rather than by what it is (e.g., as evidenced by its specific structure or specific ingredients). There is nothing inherently wrong with defining some part of an invention in functional terms. Functional language does not, in and of itself, render a claim improper. *In re Swinehart*, 439 F.2d 210, 169 USPQ 226 (CCPA 1971)."

Therefore, Applicant submits claim 40, and its dependent claims, are patentable under 35 U.S.C. §101, and definite under 35 U.S.C. §112.

C. §103 REJECTION OF THE CLAIMS

Claims 34-36, 40 and 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pare Jr. et al. (US Patent 6,269,348) in view of Glass et al. (US Patent 6,332,193).

I. *THE APPLICABLE LAW*

The Examiner has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d (BNA) 1596, 1598 (Fed. Cir. 1988). As discussed in *KSR International Co. v. Teleflex Inc. et al.* (U.S. 2007), the determination of obviousness under 35 U.S.C. § 103 is a legal conclusion based on factual evidence. See *Princeton Biochemicals, Inc. v. Beckman Coulter, Inc.*, 7, 1336-37 (Fed. Cir. 2005). The legal conclusion, that a claim is obvious within § 103(a), depends on at least four

7 Office Action at page 4.

underlying factual issues set forth in *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17 (1966): (1) the scope and content of the prior art; (2) differences between the prior art and the claims at issue; (3) the level of ordinary skill in the pertinent art; and (4) evaluation of any relevant secondary considerations.

The test for obviousness under §103 must take into consideration the invention as a whole; that is, one must consider the particular problem solved by the combination of elements that define the invention. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir.1985). The Examiner must, as one of the inquiries pertinent to any obviousness inquiry under 35 U.S.C. §103, recognize and consider not only the similarities but also the critical differences between the claimed invention and the prior art. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990), reh'g denied, 1990 U.S. App. LEXIS 19971 (Fed. Cir.1990). Additionally, critical differences in the prior art must be recognized (when attempting to combine references). *Id.* Furthermore, when determining obviousness, the Examiner:

> must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of appellant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the
> "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to "hindsight" based upon appellant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal

conclusion must be reached on the basis of the facts gleaned from the prior art.[8]

II. *DISCUSSION OF THE REJECTION OF CLAIMS 34-36, 40 AND 43-44 UNDER 35 U.S.C. §103*

Before discussing the rejections, this Response will summarize Pare and Glass.

Pare describes a system for authorizing credit and debit account transactions using biometric information instead of physical tokens, such as credit cards. Pare's point-of-sale system identifies a payer and payee. The system includes a party identification apparatus ("PIA") that receives a personal identification number ("PIN") and biometric information from the payer. The PIA sends the PIN and biometric information to a data processing center. Additionally, the PIA sends a PIA hardware identification code to the data processing center. The data processing center uses the PIN and biometric information to identify accounts associated with the payer, while using the PIA hardware identification code to identify an account associated with the payee. The PIA displays the accounts associated with the payer, and the payer selects an account from which to fund a purchase.3 Thus, Pare's system verifies payers using biometric information, and verifies payees using PIA hardware identification codes.

Glass teaches a system for securely transmitting and authenticating biometric data over a network. Glass' system includes an authentication server, camera certification authority, and a client system (e.g., personal computer) connected to a camera. Glass'

8 MPEP at § 2141.03.

system restricts access to a secured resource, such as a webpage for transferring money over a network. Upon detecting a request to access the money transfer webpage, the authentication server sends a token (e.g., a random number) to the client system, which forwards the token to the camera. In turn, the camera accepts the token. The camera captures an image, and creates a secure image by creating a digital signature for the captured image. The digital signature is based on the image, token, and a secret key known to the camera. The camera sends the secure image to the client system, which in turn forwards the secure image to the authentication server. The authentication server checks whether the secure image has been modified by re-computing the digital signature (based on the token and secret key). Next, the authentication server verifies the biometric information, and grants access to the secure resource. Thus, Glass' system verifies users based on biometric information, a secret token, a secret key, and a digital signature.

Claims 34-36 and 43-44

Claim 34 recites the following:

A computer-implemented method for verifying a user and a user computer comprising:
receiving, at a first server, a first message from the user computer, the first message including a first computer fingerprint file identifying the user computer based on information associated with a plurality of components included in the user computer;
comparing the first computer fingerprint file against a second computer fingerprint file to verify the user computer, the second computer

> fingerprint file including information associated with the plurality of components included in the user computer, and the second fingerprint file being accessible by the first server;
>
> receiving, at a second server, a second message from the user computer, the second message including a first identification for the user, the first identification being associated with the first computer fingerprint file identifying the user computer; and
>
> comparing, at the second server, the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the second mini-server; and
>
> after the comparing of the first identification for the user against the second identification for the user to verify the user, generating a third message, at the second server, based upon the results of the comparison.

As shown, the computer-implemented method of claim 34 includes operations performed by two servers. The first server receives a computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer. The first server verifies the user computer by comparing the fingerprint file against another fingerprint file. As for the second server, it receives an identification associated with the user, where the identification is also associated with the fingerprint file. The second server verifies the user by comparing the user identification with another identification associated with the user.

In rejecting claim 34, the Office Action relies on Pare's passage at column 11, lines 14-21 and 39-45. More specifically, the Office Action asserts that Pare's passage teaches the first server's receiving and comparing operations. These passages in Pare describe the identifying of parties from biometric data, a PIN, digital certificates and a PIA hardware identification code. These passages in Pare also describe a Biometric-PIN

Identification Subsystem (BPID) including a processor that receives a biometric sample and PIN, and compares the biometric sample to registered biometric samples. If there is a match, the processor transmits an identity back to a transaction processor. If there is no match, the processor transmits a "party not identified" message back to the transaction processor.

Clearly, Pare's passage does not teach a first server receiving a computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer. It is also clear that Pare's passage does not teach the first server's comparing operation. Pare does describe using a hardware security code to identify the party identification apparatus (PIA). According to Pare, an identification code is embedded, at manufacture time, in the PIA's write-once memory. As discussed above, Pare's system uses the code to identify a payee account. Therefore, Pare's use of hardware identifiers differs from claim 34's computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer.

In rejecting claim 34, the Office Action also relies on Glass' passage at column 10, lines 30-58. More specifically, the Office Action asserts that Glass' passage teaches claim 34's operations that are performed at the second server. According to the method of claim 34, the second server receives a user identification and compares the user identification to a stored user identification. In contrast, the passage from Glass describes

a computer sending an image to a server, where the image was captured by a camera connected to the computer. Along with the image, the computer sends a digital signature and camera's unique serial number to the server. The digital signature and serial number are either embedded directly into the image or alongside the image in a data packet. The server sends the serial number to a central camera certification authority which looks-up the camera's public key and returns the public key to the server. Using a token (generated earlier) and the camera's public key, the server re-calculates the digital signature to ensure the image has not been tampered with. Applicant submits that Glass' complex image authentication process does not teach or suggest claim 34's operations for verifying user identification information.

Accordingly, Applicant respectfully submits that claim 34 is patentable over the cited references. Because claims 35-36 and 43-44 depend from and further define claim 34, Applicant respectfully submits that claims 35-36 and 43-44 are patentable over the cited references.

Claim 40

Claim 40 recites the following:

A vendor computer comprising:
a first input unit configured to communicate with a first server and to receive a first server message containing information indicating that a user computer was verified by the first server based on a first computer fingerprint file identifying the user computer based on a plurality of components in the user computer;

a second input unit configured to communicate with a second server to receive a second server message containing information indicating that a user was verified, the verification being based on a first identification for the user, the first identification being associated with the first computer fingerprint file identifying the user computer;

a processor configured to receive the first server message from the first input unit and the second server message from the second input unit and to authorize an action only if both the first server message contains information indicating the user computer was verified and the second server message contains information indicating the user was verified, wherein the first server and the second server are mini-servers, and wherein the first server message and the second server message are mini-server messages.

Accordingly, claim 40 includes a first input unit configured to receive a first message indicating that a user computer was verified by the first server based on a first computer fingerprint file identifying the user computer based on a plurality of components in the user computer. Claim 40 also includes a second unit configured to receive a second message that include verification for a user, such that the verification is associated with the first computer fingerprint file identifying the user computer. Claim 40 also includes a processor to authorize action based on verification of the user computer and the user, based on these two different messages. As noted above, neither Pare nor Glass, alone or in combination, disclose or suggest these limitations.

Accordingly, Applicant respectfully submits that claim 40 is patentable over the cited references.

8. CONCLUSION

It is respectfully submitted that the claimed invention is not unpatentable in view of the cited art. It is respectfully submitted that claims 34-36, 40, and 43-44 should therefore be allowed. Reversal of the Examiner's rejections of claims 34-36, 40, and 43-44 is respectfully requested.

Respectfully submitted,

Gregg A. Peacock

DeLizio Gilliam, PLLC
15201 Mason Road
Suite 1000-312
Cypress, TX 77433
281-758-0025

Date 12/13/2010 By /Gregg A. Peacock Reg #45,001/
Gregg A. Peacock
Reg. No. 45,001

This paper or fee is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

CLAIMS APPENDIX: THE CLAIMS ON APPEAL

1-33. (Canceled)

34. (Previously Presented) A computer-implemented method for verifying a user and a user computer comprising:

receiving, at a first server, a first message from the user computer, the first message including a first computer fingerprint file identifying the user computer based on information associated with a plurality of components included in the user computer;

comparing the first computer fingerprint file against a second computer fingerprint file to verify the user computer, the second computer fingerprint file including information associated with the plurality of components included in the user computer, and the second fingerprint file being accessible by the first server;

receiving, at a second server, a second message from the user computer, the second message including a first identification for the user, the first identification being associated with the first computer fingerprint file identifying the user computer; and

comparing, at the second server, the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the second mini-server; and

after the comparing of the first identification for the user against the second identification for the user to verify the user, generating a third message, at the second server, based upon the results of the comparison.

35. (Previously Presented) A method according to claim 34, further comprising:
sending the first message to a vendor computer; and
sending the second message to the vendor computer.

36. (Previously Presented) A method according to claim 35 further comprising:
authorizing an action by the vendor computer only if both the first message contains information indicating the user computer was verified and the second message contains information indicating the user was verified.

37.-39. (Canceled)

40. (Previously Presented) A vendor computer comprising:
a first input unit configured to communicate with a first server and to receive a first server message containing information indicating that a user computer was verified by the first server based on a first computer fingerprint file identifying the user computer based on a plurality of components in the user computer;
a second input unit configured to communicate with a second server to receive a second server message containing information indicating that a user was verified, the verification being based on a first identification for the user, the first identification being associated with the first computer fingerprint file identifying the user computer;
a processor configured to receive the first server message from the first input unit and the second server message from the second input unit and to authorize an action only if both the first server message contains information indicating the user computer was verified and the second server message contains information indicating the user was verified, wherein the first server and the second server are mini-servers,

and wherein the first server message and the second server message are mini-server messages.

41.- 42. (Canceled)

43. (Previously Presented) The method of claim 34, wherein the first mini-server and the second mini-server are associated with a clearinghouse computer.

44. (Previously Presented) The method of claim 34, wherein the first mini-server is associated with a first clearinghouse computer and the second mini-server is associated with a second clearinghouse computer.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE